Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Exame de Arquitetura de Redes
24 de Junho de 2014

Duração: 2h15m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Considerando o modelo de desenho hierárquico de redes e a rede em anexo onde:
   - Em cada edifício existem 3 VLANs locais;
   - As ligações entre os switches Layer3 e os switches Layer2 dos edifícios são feitas usando ligações trunk/inter-switch que transportam todas as VLAN;
   - As ligações entre os switches Layer 3 A, B e C são feitas usando ligações Layer 3;
   - Cada VLAN nunca terá mais de 260 terminais; apenas uma VLAN necessita de 64 endereços IPv4 públicos; a rede DMZ precisa de 30 endereços IPv4 públicos;
   - Será utilizada a gama de endereços privados IPv4 10.0.0.0/16, e estão disponíveis a gama de endereços públicos IPv4 189.5.5.0/24 e a gama de endereços IPv6 2001:A1:A1::/56.

   a) Defina e atribua as sub-redes IPv4 e IPv6 necessárias (para toda a rede e seus mecanismos). (1.0 valores)
   b) Identifique os equipamentos que são um um ponto de falha crítico. Proponha soluções para aumentar a redundância e resiliência da rede nesses pontos (1.0 valores).
   c) Admitindo que se pretende criar uma rede sem fios que permite o passagem entre pontos de acesso sem perda de ligação e sem mudança de endereço IP, identifique o modelo de VLAN a implementar e defina os procedimentos para essa implementação. (3.0 valores)
   d) Após a instalação dos pontos de acesso verificou-se a existência de um número elevado de colisões, que mecanismos poderão ser ativados de modo a reduzir este problema? Justifique. (1.0 valores)
   e) Descreva os procedimentos necessários de modo a implementar uma solução de autenticação dos terminais/clientes wireless com base na norma 802.1X. (1.0 valores)

2. Admitindo que as ligações entre os switches Layer 3 A, B e C são feitas usando ligações Layer 3; que todos os switches Layer3 e routers têm os protocolos OSPFv2 e OSPFv3 ativos; que todos os interfaces têm um custo OSPF por omissão de 1; que os *routers* de acesso à Internet estão a anunciar (por OSPF) uma rota por omissão com uma métrica base de 100 (do tipo 2). Considere que a rede do "Edifício Antigo" possui um processo de RIP e que as redes IPv4 do edifício estão a ser redistribuídas sumariadas (com métrica do tipo 1 e assumindo um custo de 10) para o processo de OSPFv2 da rede principal.

   a) Escreva as tabelas de encaminhamento IPv4 e IPv6 do SWL3 A. Nota: Identifique as redes IP, endereços e interfaces por um identificador alfanumérico explícito (ex: redeIPV4vlan1.edificio1) (2.5 valores)
   b) Indique quais as configurações do OSPF a efetuar de modo a que o tráfego do edifício antigo para a rede da DMZ seja encaminhado preferencialmente pelo Router 1. (1.0 valores)
   c) Descreva uma solução que permita ao Router A começar a encaminhar o tráfego pela "ligação de último recurso" em caso de falha dos Routers 1 e 2. (1.0 valores)
   d) Explique como pode garantir que os clientes da VLAN dos terminais sem-fios nunca poderão aceder ao Datacenter. (1.0 valores)

4. a) Proponha uma possível solução de monitorização da rede que permita saber a qualquer momento o tráfego em cada um dos interfaces de todos os equipamentos de rede. (1.0 valores)
   b) Descreva que mecanismos são necessários configurar/ativar para desenvolver um sistema de alarme que notifique quando um determinado interface atingiu 80% da sua capacidade? (1.0 valores)

5. Assumindo que todas as maquinas da empresa (com endereços IPv4 privados e públicos e IPv6 globais) tem um nome associado.
   a) Indique o número, localização e configuração genérica dos servidores de DNS da empresa. (1.0 valores)
   b) Explique do ponto de vista do gestor do sistema os passos a tomar para implementar DNSSEC no(s) servidor(es) DNS da empresa. (1.0 valores).

6. Considerando a rede da figura em anexo onde os routers/SWL3 estão configurados com o protocolo OSPF (com custos iguais em todos os interfaces) e com o encaminhamento *multicast* ativo em todos os interfaces. Assuma que uma fonte S que se encontra no Datacenter envia tráfego multimédia (unidirecional) para o endereço 233.3.3.3 e que um terminal R numa VLAN do edifício 2 já aderiu à sessão multicast 233.3.3.3.
   a) Considerando que o protocolo PIM sparse-mode está ativo em todos os routers e interfaces, e que o Rendezvous-Point (RP) é um dos interfaces do SWL3 A; descreva como os primeiros pacotes enviados por S se propagam pela rede e quais os pacotes trocados entre os routers. Justifique. (1.5 valores)
   b) Considerando que um novo terminal de uma VLAN do edifício 1 quer aderir aos grupos multicast IPv4 233.3.3.3 and IPv6 FF02::3:3, o que tem o terminal de fazer para efetivar essa adesão? (1.0 valores)
   c) Suponha que se pretende garantir que o tráfego de vídeo é o mais prioritário, seguindo-se por ordem decrescente de prioridade o tráfego MySQL, HTTP e, finalmente, o restante tráfego. Explique como é que pode garantir esta política de Qualidade de Serviço em toda a rede da empresa. (1.0 valores)

Correção

1a)
- IPv4 privado:
Cada VLAN pode ter até 260 terminais (>254) logo a rede deverá ter pelo menos uma máscara de /23 (510 endereços usáveis). As ligações ponto a ponto poderão ter uma máscara /30 (2 endereços usáveis).
VLANs: 10.0.$[vvvveee0]_2$.0/23 e- edíficio (>0), v- vlan id (>0)
Ligações ponto a ponto: 10.0.0.z/30 z- múltiplos de 4

- IPv4 público:
VLAN: 64 endereços + 1 router + net id + broadcast = 67 → 128 → máscara /25 (189.5.5.0/25)
DMZ: 30 endereços + 1 router + net id + broadcast = 33 → 64 → máscara /26 (189.5.5.128/26)
NAT: alguns endereços (32 → /27) (189.5.5.192/27)
Reserva: o resto (189.5.5.224/27)

- IPv6 global (Não há IPv6 privados! Há endereços site-local mas não eram precisos neste cenário.)
Visto a máscara da rede ser /56, os primeiros 56 bits são fixos e apenas os 8 bits até à máscara /64 podem ser usados. Em VLANs para que os mecanismos stateless de atribuição de endereços funcionem a máscara tem mesmo de ser /64. Nas ligações ponto a ponto ou outras entre routers poderá usar-se outra máscara.

Endereços: 2001:A1:A1:00XX::/64, com XX de 00h a FFh.

1b) Os pontos de falha críticos são os switches de distribuição (SWL3 A e B) e o switch de core (SWL3 C) e respetivas ligações. O router A também é um ponto de falha crítico, mas assumindo que pertence a uma parte antiga da rede (inalterável) poderá permanecer sem alterações.
Solução: Colocar um switch layer3 redundante em "paralelo" com os os SWL3, A, B e C e definindo ligações redundantes entre eles.
Neste cenário: as novas ligações seriam todas layer3 com exceção das ligações entre o SWL3A e o seu redundante e entre o SWL3B e o seu redundante que seriam layer2 (trunk/inter-switch).

1c) O modelo de VLAN a usar deverá ser o "end-to-end" pois é o único que permite que os terminais possam ter o mesmo endereço IP independente da sua localização física na rede. Para a sua implementação e sabendo que as ligações entre os SWL3 A, B e C são Layer3 e não permitem o transporte de tramas Ethernet (Layer 2 VLAN traffic) de um extremo ao outro:
1- Redefinir as ligações entre os SWL3 A, B e C como ligações layer2, mudando os cabos para portas layer2 (switched) ou caso o equipamento e implementação atual o permita, por configuração/software.
2 – Definir e configurar (inclusive a rede IP) uma VLAN de interligação entre os SWL3 A, B e C e a própria VLAN para terminais sem fios.
3 – Definir as ligações entre os SWL3 A, B e C como sendo trunk/inter-swicth mas apenas com permissão para transportar as VLANs end-to-end e de interligação.
4 – Atualizar a configuração dos processos de OSPF (v2 e v3) adicionando as novas redes e definindo os interfaces das VLANs end-to-end como sendo passivos.
5 – Nos AP associar o SSID da rede sem fios à nova VLAN dos terminais sem fios e configurar um trunk entre o AP e o equipamento de ligação (SWL3 A, B ou C).

1d)
Ativação do mecanismo MACA (Multiple Access with Collision Avoidance). O MACA funciona com base nos frames RTS (Request To Send) e CTS (Clear To Send); um frame RTS é enviado pelo emissor antes de poder transmitir a pedir permissão para o fazer e o recetor envia um frame CTS quando poder receber.

1e)
É necessário implementar uma arquitetura AAA onde o AP recorre a um servidor de autenticação (RADIUS ou TACACS+). Os terminais usam protocolos de autenticações com base no EAP.

2a)
IPv4:
C RedesVLAN.Ed1 diretamente ligadas
O RedesVLAN.Ed2 (custo=3), via SWL3C //custo=1(A-C)+1(C-B)+1(B-vlan)=3
O Rede Datacenter (custo=2), via SWL3C
O Rede DMZ (custo=3), via SWL3C
O Redes C-A, C-1, C-2 (custo=2), via SWL3C
O Redes A-1, 1-2 (custo=3), via SWL3C
OE1 RedeAntiga(192.168.6.0/24) (custo=12),via SWL3C //Tipo 1 os custos internos são adicionados
OE2 RotaOmissão(0.0.0.0/24) (custo=100),via SWL3C //Tipo 2 os custos internos não são adicionados

Nota: Do ponto de vista do SWL3A, só há sempre um caminho (via SWL3 C)!

Para o IPv6 é tudo igual exceto que não há uma entrada para a rede antiga, e a rota por omissão é ::/0.

2b)
É preciso garantir que o **custo OSPF do caminho** (A-SWL3C-R2) é maior que o **custo OSPF do caminho** (A-R1-R2). Logo como os custos OSPF são todos iguais basta aumentar por exemplo o custo OSPF do interface do RA (ligado ao SWL3C) para 2 (ou qualquer coisa maior que 2). Assim o custo do caminho A-R1-R2 será 3 e o do caminho A-SWL3C-R2 será 4.

2c)
Há dois objetivos: (i) ativar a rota via ligação de recurso em caso de falha e (ii) redirecionar o tráfego de toda a rede para o RA.
(i) Definir no RA uma rota estática flutuante, ou seja uma rota estática para a rede de omissão (0.0.0.0/24) mas com uma **distância administrativa superior** ao do OSPF (o custo não interessa neste caso, visto que é uma escolha entre rotas de diferentes métodos/protocolos).
(ii) Anunciar no RA uma rota por omissão via OSPF para o core da rede com um **custo** superior (depende do tipo de métrica mas convém ser muito maior) ao anunciado pelos Router 1 e 2 (neste caso >100).

2d)
Definindo uma ACL (ou qualquer regra de filtragem) no interface do SWL3C que liga ao Datacenter (no sentido do Datacenter) que bloqueie todos os pacotes com IP de origem da VLAN wireless.
Nota: Pode ser feito também nos APs ou nos SWL3 distribuição ou core, bloqueando todo o tráfego com IP de origem da VLAN wireless e IP de destino do Datacenter. Esta solução evita que o tráfego chegue ao core, mas é muito mais complexa.

4a)
Configuração do SNMP em todos os equipamentos da rede, que passarão a ser agentes SNMP, e definição de comunidades. Através de um script, é possível ler a informação das MIBs dos equipamentos, nomeadamente o tráfego em cada um dos seus interfaces (pooling).
Esta monitorização deve ser feita recorrendo a VLAN end-to-end.

4b)
É necessário ativar e configurar SNMP Traps em todos os equipamentos de rede. Permitem que os agentes SNMP enviem notificações sempre que um dado evento ocorre, neste caso, quando o tráfego num interface atinge 80 da sua LB.
Outra opção é fazer polling contínuo de todos os equipamentos, detetando as interfaces cujo tráfego ultrapassa 80% da sua LB.

5a)
A empresa deverá ter dois servidores DNS, um público e um privado.
O servidor privado deve estar localizado numa rede sem acesso do exterior e ligada à camada de core, de modo a minimizar o tempo médio de acesso por parte de todos os equipamentos da rede.

O servidor público deve estar localizado numa rede com acesso a partir do exterior e o mais próxima possível dos routers do ISP, como por exemplo a DMZ.
O servidor DNS público contém registos do tipo A, que permitem fazer a tradução de um nome num endereço IPv4 das máquinas com endereços públicos, registo do tipo AAAA, que permitem fazer a tradução de um nome num endereço IPv6 das máquinas com endereços globais. Contém ainda um registo NS que identifica o nome do servidor DNS público, um registo do tipo A que identifica o endereço IPv4 do servidor DNS público a partir do nome e um registo AAAA que identifica o endereço IPv6 do servidor DNS público a partir do nome.
O servidor DNS privado contém todos os registos do servidor público e ainda todos os registos do tipo A para todas as máquinas com endereços privados.

5b)
Cada servidor DNS deve

- criar dois pares de chaves pública-privada, uma chave para assinar os registos DNS (a ZSK) e outra para assinar as assinaturas dos registos DNS (a KSK).
- colocar as chaves públicas no ficheiro da respetiva zona (DNSKey);
- criar os registos RRSIG que contêm a chave privada (permitindo verificar a veracidade e integridade dos registos DNS);
- criar os registos DS e DLV; colocar os registos DS na zona pai e os DLV num servidor central da Internet. Estes registos permitem a verificação das chaves de uma zona filha e a criação de uma cadeia de confiança.

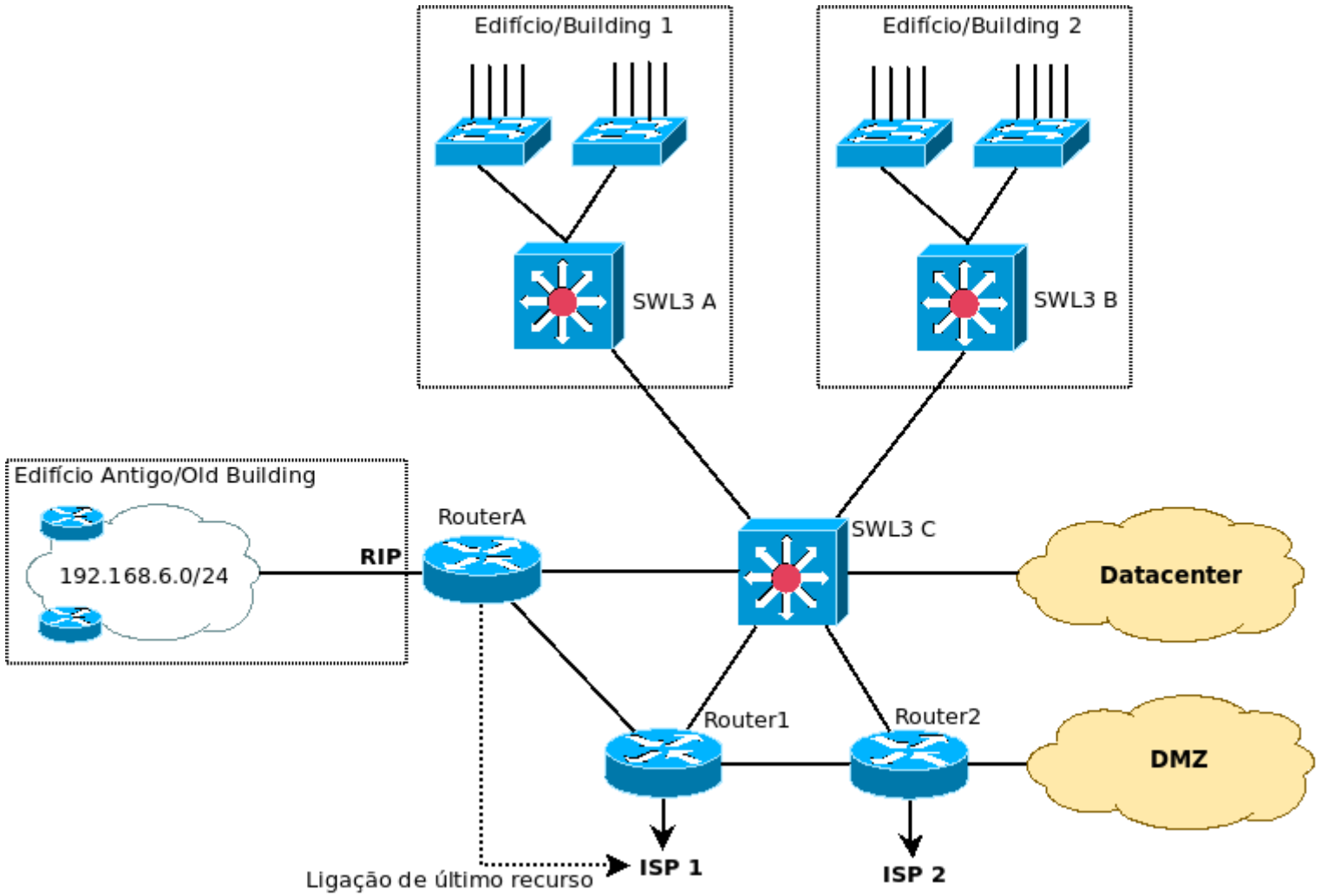
6a)

- a fonte S envia um pacoite multicast em unicast para o RP através de uma mensagem Register;
- o SWL3A (RP) ao receber o Register recupera o pacote multicast e encaminha-o pela group-shared tree para o cliente R;
- o RP envia um Join para a fonte S para estabelecer uma source-based tree;
- a fonte S, ao receber o Join, envia pacotes multicast nativos, para além dos pacotes encapsulados;
- o RP, ao receber o pacote multicast nativo, envia para a fonte S uma mensagem Register-Stop;
- a fonte S ao receber a mensagem Register-Stop passa a enviar apenas pacotes multicast nativos, estando estabelecida a source-based tree;
- eventualmente, o SWL3B verificará que tem um caminho mais curto para a fonte que não passa pelo RP e enviará um Join para o SWL3C e um Prune-RT para o RP (SWL3A).

6b)
O terminal enviará um IGMP Membership Report para indicar que pretende aderir ao grupo multicast IPv4 233.3.3.3 e um Multicast Listener Report para indicar que pretende participar na sessão multicast FF02::3:3

6c)
Política de QdS baseada na arquitetura DiffServ.
Em primeiro lugar, temos que definir as classes de tráfego, como por exemplo: vídeo EF, MySQL AF11, HTTP AF22 e restante tráfego DE.
Os router fronteira (Routers 1 e 2 e switches L3 A e B) são responsáveis pela marcação dos pacotes no campo DSCP (nos interfaces de entrada). Nos interfaces de saída são aplicadas políticas de QdS apropriadas (por exemplo, atribuíndo uma percentagem de LB adequada a cada uma das classes de tráfego).
Nos routers de core são apenas aplicadas políticas de QdS apropriadas.
A identificação dos pacotes é normalmente feita recorrendo a ACLs.

Nome:_____ Número:_____


Edifício/Building 1
Edifício/Building 2
SWL3 A
SWL3 B
Edifício Antigo/Old Building
192.168.6.0/24
RIP
RouterA
SWL3 C
Datacenter
Router1
Router2
DMZ
ISP 1
ISP 2
Ligação de último recurso